Многочлены и теория чисел

Показатель, к которому принадлежит вычет

Пусть $p \in \mathbb{P}$, $a \in \mathbb{Z}_p$, $a \neq 0$, $d \in \mathbb{N}$. Вычет принадлежит к показателю d, если $a^d = 1$, но $a^s \neq 1$ при $s \in \mathbb{N}, s < d$. Обозначение: $a \underset{p}{\in} d$

Лемма 1

Пусть $p \in \mathbb{P}$, $a \in \mathbb{Z}_p$. Тогда выполнены следующие утверждения:

1. Если $a^d = 1$ и $a \underset{p}{\in} s$, то $s \mid d$.
2. Если $a \underset{p}{\in} d$, то $d \mid p - 1$

Лемма 2

Если $p \in \mathbb{P}$ и $d \mid p - 1$, то многочлен $t^d - 1 \in Z_p[t]$ имеет ровно d корней, и все они не 0.

Теорема 1

Если $p \in \mathbb{P}$ и $d \mid p - 1$, то к показателю d принадлежит ровно $\varphi(d)$ вычетов.

Первообразный корень по модулю p

Пусть $p \in \mathbb{P}$. Вычет $a \in \mathbb{Z}_p$ - первообразный корень по модулю p, если $a \underset{p}{\in} p - 1$. По теореме 1 существует в точности $\varphi(p - 1)$ первообразных корней по модулю p.

Теорема 2

Пусть $p \in \mathbb{P}$, а a - первообразный корень по модулю p. Тогда $a, a^2, ..., a^{p-1} = 1$ - ПрСВ (mod p), то есть, в точности все ненулевые вычеты из $\mathbb{Z}_p$.

Квадратичный вычет и невычет в $\mathbb{Z}_p$

Пусть $p \in \mathbb{P}$, $a \in \mathbb{Z}_p$, $a \neq 0$.

- Тогда a - квадратичный вычет, если сущестует такой $b \in \mathbb{Z}_p$, что $b^2 = a$.
- Если такого b не сущесвует, то a - квадратичный невычет.

Лемма 3

Пусть $p \in \mathbb{P}$, $p_1 := \frac{p-1}{2}$. Тогда:

1. квадратичные вычеты в $\mathbb{Z}_p$ - корни многочлена $t^{\frac{p-1}{2}} - 1$;
2. если $x^2 = y^2$, то x = y или x = -y;
3. существует в точности $\frac{p-1}{2}$ квадратичных вычтов в $\mathbb{Z}_p$

Лемма 4

Пусть $p \in \mathbb{P}$. Тогда выполнены следующие утверждения:

1. Квадратичный невычет в $\mathbb{Z}_p$ корни многочлена $t^{\frac{p-1}{2}} + 1$.
2. Существует в точности $\frac{p-1}{2}$ квадратичных невычето в в $\mathbb{Z}_p$.

Решение квадратных уровнений в $\mathbb{Z}_p$

- Если D - квадратичный вычет, то $D = d^2$ для некоторого $d \in \mathbb{Z}_p$ и $\frac{D}{4a^2} = \left(\frac{\pm d}{2a}\right)^2$. Тогда уравнение имеет два решения: $x_{1,2} = \frac{-b \pm d}{2a}$.
- Если D = 0, то уравнение имеет одно решение $x_1 = \frac{-b}{2a}$.
- Если D - квадратичный невычет, то $\frac{D^2}{4a^2}$ - квадратичный невычет, а значит, решений нет

Символ Лежандра

Пусть $p \in \mathbb{P}, a \in \mathbb{Z}, a \not\vdots p$.

- Тогда a - квадратичный вычет по модулю p, если a в $\mathbb{Z}_p$ - квадратичный вычет
- Аналогично для невычета

Символ Лежандра определение

Пусть $p \in \mathbb{P}, a \in \mathbb{Z}$

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ , если a - квадратичный вычет по модулю p} \\ -1 \text{ , если a - квадратичный невычет по модулю p} \\ 0 \text{ , если a} \vdots p \end{cases}$$

Свойство 1

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (\mathrm{mod}\, p)$$

Свойство 2

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}}$$

Свойство 3

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$$

Лемма 6

Пусть $p \in \mathbb{P}, a \in \mathbb{Z}, a \not\vdots p$.

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{\frac{p-1}{2}} \left[\frac{2ax}{p}\right]}$$

Лемма 7

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Теорема 3 (закон взаимности Гаусса)

$p, q \in \mathbb{P}, p \neq 2, q \neq 2$. Тогда:

$\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$

Кольцо многочленов $\mathbb{Z}[t]$. Соедержание многочлена.

Пусть $f(t) = a_n t^n + ... + a_0 \in \mathbb{Z}[t]$. Тогда его **содержание** $c(f) = (a_0, ..., a_n)$.

Лемма 8 (лемма Гаусса)

Пусть $f, g \in \mathbb{Z}[x], c(f) = c(g) = 1 \Rightarrow c(fg) = 1$

Следствие 1

Для $f, g \in \mathbb{Z}[x]$ выполнено $c(fg) = c(f)c(g)$

Связь неприводимости в $\mathbb{Q}[x]$ и $\mathbb{Z}[x]$

Если многочлен $f \in \mathbb{Z}[x]$ неприводим в $\mathbb{Q}[x]$, то он, очевидно, неприводим и в $\mathbb{Z}[x]$.

Основная теорема арифметики в $\mathbb{Z}[t]$

Многочлен $f \in \mathbb{Z}[t]$ - **тривиальный**, если $c(f) = 1$.

Теорема 4

Любой многочлен $f \in \mathbb{Z}[x]$ с положительным старшим коэффициентов расскладывается в произведение $f = r_1...r_k \cdot p_1...p_n$, где $r_1, ..., r_k \in \mathbb{P}$, а $p_1, ..., p_n \in \mathbb{Z}[x]$ - тривиальные неприводимые многочлены с положительными старшими коэффициентами. Разложение единственно с точностью до перестановки сомножителей.

Критерий Эйзенштейна

Теорема 5

Пусть $f(x) = a_n t^n + ... + a_1 t + a_0 \in \mathbb{Z}[t]$ и $p \in \mathbb{P}$ таковы, что $a_n \not\vdots p, a_{n-1}, ..., a_0 \vdots p$ и $a_0 \not\vdots p^2$. Тогда f - неприводим в $\mathbb{Z}[x]$.

Следствие 3

Пусть $f(x) = a_n t^n + ... + a_1 t + a_0 \in \mathbb{Z}[t]$ и $p \in \mathbb{P}$ таковы, что $a_0 \not\vdots p, a_1, ..., a_n \vdots p$ и $a_n \not\vdots p^2$. Тогда f - неприводим в $\mathbb{Z}[x]$.

Значения в целых точках многочлена из $\mathbb{Z}[t]$

Лемма 10

Пусть $f(x) = a_n t^n + ... + a_1 t + a_0 \in \mathbb{Z}[t], x, y \in \mathbb{Z}, x \neq y \Rightarrow f(x) - f(y) \vdots x - y$.

Разностный многочлен

Пусть $f \in K[x]$, где K - коммутативное кольцо с 1, причем $\mathbb{Z} \subset K$

Разностный многочлен

$$\Delta f(x) \coloneqq f(x+1) - f(x)$$

Лемма 13

Пусть $f \in K[x]$, где K - коммутативное кольцо с 1, причем $\mathbb{Z} \subset K$. Тогда
$\Delta f \in K[x], \deg\ (\Delta f) = \deg(f) - 1$